

FILED  
JAN 22 2025

## UNITED STATES DISTRICT COURT

for the  
Northern District of OklahomaHeidi D. Campbell, Clerk  
U.S. DISTRICT COURT

In the Matter of the Search of )  
 Information Associated with Kik Username: ) Case No. 25-mj-32-JFJ  
 'james2684321' that is Stored at a Premises )  
 Controlled by MediaLab.ai, Inc. )

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

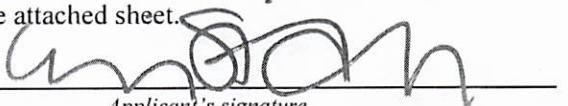
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § §§ 2252(a)(4)(B) and 2252(b)(2)	Possession of Child Pornography
18 U.S.C. §§ 2251(a) and 2251(e)	Production of Child Pornography

The application is based on these facts:

See Affidavit of Erin Staniech, attached hereto.

- Continued on the attached sheet.
- Delayed notice of \_\_\_\_\_ days (give exact ending date if more than \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

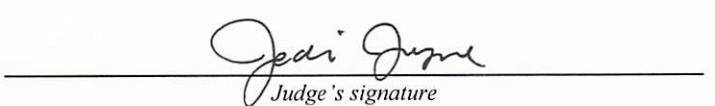
  
Applicant's signature

Erin Staniech, SA HSI

Printed name and title

Subscribed and sworn to by phone.

Date: 1/22/25

  
Judge's signature

Jodi F. Jayne, U.S. Magistrate Judge

Printed name and title

City and state: Tulsa, Oklahoma

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of  
Information Associated with Kik  
Usernames: ‘james2684321’ that is  
Stored at a Premises Controlled by  
MediaLab.ai, Inc.**

Case No. \_\_\_\_\_

**Affidavit in Support of an Application for a Search Warrant**

I, Erin Staniech, being duly sworn, depose and state:

**Introduction and Agent Background**

1. I make this affidavit in support of an application for a search warrant for information associated with Kik username ‘james2684321’ that is stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab.ai, Inc. to disclose to the government records and other information in its possession, pertaining to the individuals associated with **Kik username ‘james2684321’**, (hereinafter the “**SUBJECT ACCOUNT**”).

2. I have been employed as a Special Agent with Homeland Security Investigations (HSI) since 2019. I am currently assigned to the Office of the Resident

Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography.

3. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) twelve-week 'Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2251 and 2252.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because I submit this affidavit for the

limited purpose of showing probable cause, I have not included each fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue the requested warrant and I have not set forth all my knowledge about this matter. Additionally, unless indicated otherwise, all statements and conversations described herein are related in substance and in part only, rather than verbatim.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Children) have been committed by the individuals associated with the **SUBJECT ACCOUNT**. There is also probable cause to search the information described in Attachment A for evidence of this crime and contraband or fruits of this crime as described in Attachment B.

#### **Jurisdiction**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **Probable Cause**

7. On December 18, 2024, Homeland Security Investigations (HSI) Tulsa investigators received information that a person in the Northern District of

Oklahoma was engaging in sexual communication with a person he believed was a father of an 8-year-old girl. The father is an online undercover persona of an HSI special agent, herein referred to as UC, currently assigned to the HSI Detroit office.

8. On December 17, 2024, during an ongoing undercover child exploitation operation, the UC joined the groups #familyinsect on the application Kik. The UC observed that Kik user **james2684321** was also a member of this group, and when another member asked “Who are you into?” Kik user **james2684321** stated whole family”. In a post in this group on December 18, 2024, Kik user **james2684321** stated that he was a 40-year-old male from Oklahoma.

9. On the same day, Kik user **james2684321** send a private message to the UC. The following is an excerpt of the messages privately exchanged between the UC and Kik user **james2684321**:

- **james2684321:** 8
- UC: yes
- **james2684321:** Active
- UC: Yep
- **james2684321:** Samewith mine 11 10.7
- UC: mmmmm really?
- UC: Girls? Boys?

- **james2684321:** G
- **UC:** How active
- **james2684321:** Eleven year old aural, and I can get have my head in ten year old oral only and finger again. Seven year old just started playing with her pussy
- **UC:** Mmmm ever show em off
- **james2684321:** Only one naked pic of 10 year old u
- **UC:** Pics of me and Hailey together 

10. At this point in the conversation, Kik user **james2684321** sent a photo of a prepubescent female standing in what appears to be a living room. The female is nude with only a towel around her shoulder draped down her side. The female's vagina is visible.

11. The conversation continues:

- **UC:** Mmmm damn how old is that
- **james2684321:** 10
- **UC:** No I mean how long ago did you take the pic haha
- **james2684321:** 3 months
- **UC:** she have any idea you took a pic [devil emoji]
- **james2684321:** No
- **UC:** Hehehe you show her off lots?
- **james2684321:** No

- UC: [shush emoji] I won't tell
- UC: What's her name
- **james2684321**: Jamie
- UC: Haha I like the edited pic in your gallery
- UC: What made you do that [laughing emoji]
- **james2684321**: I had a friend and then I was trying to get him to

send me pictures of his daughter. So he wanted to see mine, but I did that to entice him. Can I see your picture now

- UC: Yeah but do you have a normal pic of her so I know she's yours and not just a pic you found

- **james2684321**: Ok
- User **james2684321** sends a family photo consisting of an adult male, adult female, and three minor females.

- **james2684321**: Family pic
- UC: Which one is Jamie
- **james2684321**: Middle
- UC: What's the dirtiest vid you have
- UC: Like not of her but at all haha
- **james2684321**: A mom licking her baby's pussy
- **james2684321**: U
- UC: Mmmm really??

- UC: I have me and Hailey just don't wanna get always super cautious for THAT to get out
  - james2684321: I am too
  - james2684321: But I did send a pic of my dau
  - james2684321: But I understand if you don't want to no pressure
  - UC: You ever vid you and her together
  - UC: You don't have to send just asking
  - james2684321: Not yet
  - UC: Do anything to them while they sleep?
  - james2684321: if i'm really high
  - UC: [sweat emoji] like what
  - james2684321: Lick there pussys licker and little then i stop
  - UC: [sweat emoji] [sweat emoji] [devil emoji] ever record any of that
    - james2684321: No
    - UC: I gotcha
    - james2684321: I'm sorry. I'm just starting to do stuff with them and starting to get pictures and everything its slow going because I don't want to scare them off
    - UC: No I gotcha

- **james2684321**: I would really love to see the picture of you two together
- UC: All depends on how dirty your stuff gets...[devil emoji]

12. User **james2684321** sends three videos:

a. Video 1: The video is 1:02 in length. The video begins with an adult female lifting the legs of a prepubescent female. The female is nude from the waist down and her anus is visible. The adult female can be seen spreading the prepubescent female's vagina and showing it to the camera. The adult female then spits on the prepubescent female's vagina and performs oral sex. At approximately 38 seconds, the adult female pulls the prepubescent female closer to the camera. The adult female can be seen spreading the vagina and the cheeks of the buttocks, exposing the anus, of the prepubescent female. The adult female continues to perform oral sex on the prepubescent female. At approximately 1:48, the adult female uses her fingers to rub the anus and vagina of the prepubescent female. The video ends with the adult female reaching towards the camera.

b. Video 2: The video is approximately 18seconds in length. The video shows a prepubescent female sucking on an erect, adult male penis. The adult male's hand is wrapped around the shaft of the

penis masturbating. At approximately 3 seconds, the female's hand wraps around the shaft of the penis and moving up and down.

c. Video 3: The video is approximately 40 seconds in length and the words "telegram: @temykab907" can be seen printed in red at the bottom right of the video.

13. The conversation continues:

- **james2684321:** Can I see
- **UC:** Yeah
- **UC:** When's the last time you played with your daughter
- **james2684321:** Week
- **UC:** Which one
- **UC:** How much did you do
- **james2684321:** I play with my oldest more. My middle daughter only sucks my Dick and I eat and finger her in my 7-year-old. I only finger her, Has she plays with my dick
- **UC:** Wowwwww
- **UC:** Wife have any clue
- **james2684321:** No
- **james2684321:** Can I see u 2 lol
- **UC:** Think she'd be down? Or go nuts haha
- **UC:** Yeah lemme find it

- UC: Who was the last daughter you got to play with
- **james2684321:** Well, I plan on fucking. All 3 of them just gotta go slow. With each of them get, I'm used to it. That's what I did with my oldest. When she was younger, just hatter play with my Dick, I played with her, got my wife's toy. Started using it on her little-by-little. Make her start sucking me. Made myself start eating her. Just went on from there until onto the point. Now we're all my head can fit in.

- **james2684321:** Last daughter was the oldest Last night
- UC: Wowwww what are the other two names
- **james2684321:** I'll tell you after resend it
- UC: Fair enough
- UC: You get to play a lot? I have to sneak and wife is always around
- **james2684321:** My wife works nights so I get to every night
- UC: The girls know about each other??
- **james2684321:** No
- UC: How come
- **james2684321:** Hotter
- **james2684321:** We're going to get caught, which makes them more nercous and more scared and turns them on more
- UC: Hehe you scare them?

- **james2684321:** Flight They enjoy having fun but they're scared.

One of their sisters got to find out where mom's gonna find out. Or if one of the cats make a noise while we're playing, they're scared, which turns me on interest me them to

#### **Identification of james2684321**

14. On December 17, 2024, HSI Detroit send an emergency request to Media Lab, LLC for the Kik username **james2684321**. Media Lab responded with the following subscriber information:

- d. Date: December 17, 2024
- e. First Name: **james2684321**
- f. Last Name:
- g. Email: [brad\\_friend@yahoo.com](mailto:brad_friend@yahoo.com) (unconfirmed)
- h. Username: **james2684321**
- i. IP: 2024/12/16 13:18:44 UTC 1734355124357 CAN  
"ip":"107.19.0.147"

15. HSI Detroit identified IP address "107.19.0.147" belonged to ATT and contacted them. ATT stated the IP address was assigned to Walmart and could not be attributed to a particular individual.

16. HSI Detroit located the IP address 2024/12/16 23:30:35 UTC  
"ip":"98.97.86.175", "Port": "31632" and identified it as belonging to Starlink. HSI Detroit contacted Starlink who provided the following information:

- j. Contact Type: Main
- k. Contact Name: Bradley Friend
- l. Contact Email: friendbrad2684@yahoo.com
- m. Contact Phone: +19183706458

SERVICE ADDRESS:

n. Address: 6600 E 390 Rd apt 36, Oologah, OK 74053,

USA

o. Address Lat: 36.4519321

p. Address Long: -95.7118644

q. Address Country: United States US

<http://maps.google.com/maps?t=m&q=loc:36.4519321+-95.7118644>

17. HSI Detroit contacted Yahoo regarding the email address friendbrad2684@yahoo.com. Yahoo responded with the following information:

Attribute Value

r. Other Identities

s. brad\_friend

Mail Name

t. brad\_friend@yahoo.com

u. Account Status: active

v. Registration IP Address:

2600:1700:9800:db90:50e8:22c1:2793:d49d

w. Registration Date: 2019-06-13T03:55:43.000Z

x. Full Name: Brad Friend

18. Further, Yahoo provided IP addresses for the user between the dates December 4th and December 18, 2024. Agents located the same IP address used to register the Kik account.

19. Further, an HSI Criminal Analyst conducted an open source search for the phone number 9183706458 and identified the number as belonging to Bradley Schutt in Oologah, Oklahoma.

20. Upon receipt of the information HSI Tulsa special agents located a driver's license for Bradley Schutt. The driver's license photo matched the adult male in the family photo that was sent by SCHUTT in Kik. The address on the driver's license matches the Subject Residence.

21. Additionally, I located a marriage license for SCHUTT and Christi Friend who were married in April of 2014.

22. I searched Facebook and located a profile for Christi Friend. I reviewed the photos within her profile and located the same family photo sent by SCHUTT to the UC in the Kik chat.

23. The Honorable Susan Huntsman authorized a criminal complaint and arrest warrant for SCHUTT on December 18, 2024, case 24-MJ-799-SH.

24. The Honorable Susan Huntsman authorized a search warrant for the person and house of Bradley SCHUTT, case 24-MJ-800-SH.

25. The Honorable Jodi F. Jayne authorized a search warrant for SCHUTT's cellular device, case 24-MJ-805-JFJ.

26. SCHUTT gave a post Miranda interview and clarified that his legal name is now Bradley FRIEND, because he took his wife's name after they got married.

**Background on Kik and MediaLab.ai, Inc.**

27. Kik is owned and operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik Messenger allows users to "talk to your friends and browse and share any web site with your friends on Kik." According to their website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

28. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

29. In general, providers like Kik ask their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, Kik does not verify that information. Kik also retains certain transactional information about the creation and use of each account on their systems, including the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

30. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

31. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e. a phone number), it has become a popular app used by people involved in the collection, receipt, and distribution of child pornography.

32. In my training and experience, an application user's IP log, stored electronic communications, and other data retained by the provider, can indicate who has used or controlled the application account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and

tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Kik account at a relevant time. Further, Kik account activity can show how and when the account was accessed or used. For example, as described herein, Kik logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik access, use, and events relating to the crime under investigation. Additionally, Kik account activity may provide relevant insight into the Kik account owner's state of mind as it relates to the offense under investigation. For example, information on the Kik account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Therefore, the computers and systems of Kik, owned and operated by MediaLab.ai, Inc., are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Kik, such as account access information, transaction information, and other account information.

#### **Characteristics Common to Individuals Who Exhibit a Sexual Interest in**

##### **Children**

34. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children, and who distribute, receive, possess, and/or access with intent to view child pornography:

- i. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- ii. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;
- iii. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals

who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

iv. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, on their person, to enable the individual to view the child pornography images, which are valued highly. Such individuals do not like to be away from their child pornography images for an extended period of time. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

v. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

vi. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly,

such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared; and

vii. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

**Information to be Searched and Things to be Seized**

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab.ai, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **Conclusion**

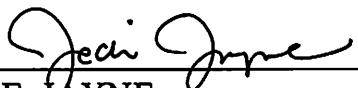
36. Based upon the facts set forth in this affidavit, I believe that there is probable cause to believe that the location described in Attachment A contains evidence of violations of Title 18, United States Code, Sections 2251 and 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Children).

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on MediaLab.ai, Inc. Because the warrant will be served on MediaLab.ai, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,

  
Erin Staniech  
Special Agent  
Homeland Security Investigations

Subscribed and sworn by phone on January 22, 2025

  
\_\_\_\_\_  
JODI F. JAYNE  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to be Searched**

This warrant applies to information associated with the account associated with Kik usernames ‘james2684321,’ (SUBJECT ACCOUNT), that are stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a company headquartered at 1222 6th Street, Santa Monica, CA 90401.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by MediaLab.ai, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab.ai, Inc., regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab.ai, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab.ai, Inc. is required to disclose the following information to the government for each account listed in Attachment A:

- (a) All contact and personal identifying information;
- (b) All activity logs for the account and all other documents showing the user's posts and other Kik activities;
- (c) All photos and videos uploaded by the SUBJECT ACCOUNT and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Kik usernames; groups and networks of which the user is a member; future and past event postings; rejected

“Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of MediaLab.ai, Inc.’s applications;

- (e) All basic subscriber information,
- (f) All call detail records,
- (g) All detailed message logs,
- (h) All content, including but not limited to message content,
- (i) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (j) All other records and contents of communications and messages made or received by the user, including all Messenger activity, messages, chat history, video and voice calling history, and pending “Friend” requests;
- (k) All “check ins” and other location information;
- (l) All IP logs, including all records of the IP addresses that logged into the account;
- (m) All past and present lists of friends created by the account;
- (n) All records of Kik searches performed by the account;
- (o) The types of service utilized by the user;

- (p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (q) All privacy settings and other account settings, including privacy settings for individual Kik posts and activities, and all records showing which Kik users have been blocked by the account;
- (r) All records pertaining to communications between MediaLab.ai, Inc. and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252 for the **SUBJECT ACCOUNT**, listed on Attachment A, including:

- (a) Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;
- (b) Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission,

through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

- (c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- (d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and
- (e) The identity of the person(s) who created or used the SUBJECT ACCOUNT including records that help reveal the whereabouts of such person(s).
- (f) Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including,

but not limited to:

- i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;
- ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and
- iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.